Working Memo 868

DATE: August 26, 2003

TO: ODW Professional Staff

THROUGH: Robert B. Taylor, P.E., Director
Office of Drinking Water

FROM: Mark C. Anderson, Technology Transfer Director
Office of Drinking Water

SUBJECT: Water – Emergency Response – Vulnerability Assessments and VSAT™

Background

The water infrastructure is one of the original eight critical infrastructures identified in Presidential Decision Directive 63. Presidential Decision Directive (PDD) 63 issued on May 22, 1998, calls for "...vulnerability assessments...for each sector of the economy and each sector of the government that might be a target of infrastructure attack intended to significantly damage the United States...", and "...within both the government and the private sector to sensitize people to the importance of security and to train them in security standards..." The President designated the United States Environmental Protection Agency (EPA) as the lead federal agency (LFA) to protect water infrastructure security.

Concern for this critical infrastructure extends to the US Congress. In enacting the Bioterrorism Act of 2002, Congress amended the Safe Drinking Water Act (SDWA). Community waterworks serving populations over 3,300 are required by Congress to conduct vulnerability assessments. Small systems (serving populations between 3,301 and 49,999) have until June 30, 2004, and medium systems (populations between 50,000 and 99,900) have until December 31, 2003, to complete vulnerability assessments. Large drinking water systems serving populations over 100,000 have until March 31, 2003. Within six months of submitting their vulnerability assessments to the Environmental Protection Agency, waterworks must furnish EPA a certification that an emergency response plan has been prepared or revised to address topics of concern identified by EPA.

Currently, the primacy agency for security provisions of the SDWA is the Region III Office of the EPA. Headquarters EPA will approve the vulnerability assessments, but the Region can have one employee review the assessments (once obtaining the appropriate security clearance).

Vulnerability assessments can be conducted by using several available methodologies. The

Association of Metropolitan Sewerage Agencies (AMSA) developed tools to assist wastewater utilities conduct vulnerability assessments. One is a detailed, asset based vulnerability checklist and the other is a software tool that provides a systemic approach to identifying, organizing, documenting, and presenting complex information in a clear and logical manner. Called VSAT™ for Vulnerablity Self Assessment Tool the software supports waterworks, wastewater works, and combined service authorities with three tailored versions. Because it saves input to a database, all entries are retrievable, and has strong financial tools that no other methodology has, it is the preferred methodology.

Any vulnerability assessment methodology can be used that meets the six criteria established by EPA in its guidance to waterworks. The complete description of the requirements can be found in EPA's guidance, but briefly they are:

1) Characterize the water system, including its mission and objectives
2) Prioritize adverse events/ consequences to avoid
3) Determine critical assets that might be subject to malevolent acts that could result in undesired consequences
4) Assess the likelihood (qualitative probability) of such malevolent acts from adversaries
5) Evaluate existing countermeasures
6) Analyze current risk and develop a prioritized plan for risk reduction

The Terrorist Threat

The last few years witnessed both the intent and capability of international terrorism to increase the scale of consequences of its attacks. An attack on the US water infrastructure by a terrorist organization is feasible in principle and a real threat in practice. Multiple terrorist objectives are likely in executing such an attack, yet achieving any objective would represent success. In theory, the deliberate tampering of US water supplies by a terrorist organization might meet the quest for increased scale.

In this operational construct, the media is the terrorist's greatest ally and conversely, a grave threat. The terrorist organization wants media coverage of every one of its successes and every failure to pass with little or no comment. So one can assume the scale will be large enough to warrant media coverage especially among the cable news channels.

In terrorist operations against economic targets, the attack does not have to be 100% successful to impact business confidence. That the attack has taken place is impact enough. Obviously, the level of success increases the impact, but every attack, no matter its level of success, will impact the overall situation. Waging a campaign against economic targets differs greatly from waging a campaign against military ones. An economic campaign could achieve its effect by what could be described as "sporadic economic vandalism." Any organization, any group or disgruntled individual can join in at any time and any place. This is smart terrorism at its most dangerous and devising countermeasures is extremely difficult.

Characteristics of smart terrorism include:

- Focused terrorist strikes aimed at inflicting maximum effect in terms of loss of human life and economic cost
- A strategic concentration on the threat of, or the use of, weapons of mass destruction (WMD)
- Tactical strikes to create diversions from the WMD threat
- Decentralized, networked terrorist organizations
- Sources of financial and technical support, whether government or non-state actors, which have plausible deniability
- Maintenance of momentum, in the event of successful counter-terrorist activity, by commencing a new operation. (The effect of this is to keep anti-terrorist forces in constant uncertainty and at full alert.)

Terrorist Targets

To be really worthwhile, targets should have a high visibility and be easy to attack (soft). Attacking well defended (hard) targets increases the chance of failure and the resultant negative press. Target intelligence and reconnaissance is the key and, where possible, intelligence collection and reconnaissance will take place over weeks rather than days. A well orchestrated terrorist attack will generate a ripple effect throughout the US culture, as seen with the attacks of 9/11. Various groups would operate against targets in the following sectors:

- Political.
- Economic.
- Technological.
- Social. This sector would include **drinking water**.
- Military.

Terrorism and the Water Infrastructure

If the objectives of terrorism is to disrupt society, destroy the US economy, and the create fear, then our water infrastructure could be targeted readily. Wastewater and waterworks assets are easy targets and not particularly protected, yet hazardous chemicals are delivered, stored, and used on site. Additionally, wastewater gravity sewers could provide covert access to other key assets and critical buildings. Threats to the environment and public health are real. Wastewater treatment plants are upstream of many raw water intakes.

Security threats from terrorist and related events are relatively new to the water infrastructure, so industry-wide, standard protocols are developing. Serious security practices have evolved out of the water industry, such as with high-risk government buildings, nuclear power plants, and airline terminals. Water infrastructure physical assets are typically dispersed, so, standard approaches to security (developed for enterprises with highly centralized assets, such as dams or

nuclear weapons production facilities) are difficult to apply. Managers must then face a balancing act between demands for security and the resources needed to enact and finance those actions.

The Association of Metropolitan Sewage Agencies (AMSA), developed a methodology to conduct vulnerability assessments adopting a different approach to security for the water infrastructure tan traditionally used in other industries. AMSA brought together subject matter experts that developed an asset based vulnerability assessment checklist. The value of this product is that it is asset based. Focusing on assets, and not the probability of an attack, enables us in the water industry to assess better our vulnerabilities without needing detailed threat assessments.

The AMSA team identified five categories of assets — physical assets, the information technology (IT) platform, employees, the knowledge base and customers.

PHYSICAL ASSETS include

- Raw water sources
- Treatment plant and processes
- Perimeter control
- Control of entry/access to facilities
- Site and facility surveillance
- Vehicle and materials delivery management
- Collection system
- Distribution system
- Hazardous material control

Although assets to us in the drinking water and wastewater industries, some of the assets represent threats as well. If international terrorist organizations intend to use the infrastructure against us, the water infrastructure in the US provides that opportunity. The bulk delivery and storage of hazardous chemicals, such as elemental chlorine and ammonia, represent a weakness that can be exploited. Fortunately, over recent years a lot has been accomplished in the control of hazardous materials. But still many facilities in Virginia have railcars and one-ton cylinders of elemental chlorine and bulk storage of ammonia on site. *Note: A wastewater works collection system offers access to other facilities — not just to the publicly owned treatment works (POTW).*

Deliveries to treatment plants are not only chemicals, but deliveries of spare parts, express mail, and contractor parts and equipment. Access to the facility may include tour groups, contractor personnel, media personnel, and inspectors from state and federal agencies. Imagine the opportunity presented to a potential terrorist for access to a large POTW by the number of trucks entering and exiting a day just to remove biosolids. Also, how access is controlled at remote

sites such as water storage tanks that might have microwave and other antennae situated on top need addressing.

Raw water sources may be hard to secure, but difficult to contaminate. Raw water intakes, transmission lines, and pumps are easier targets to attack and their loss would disrupt production. Contamination of raw water promises the terrorist a low probability of success because of dilution and the treatment processes that follow.

INFORMATION TECHNOLOGY (IT) assets include:
- Internet policies and planning
- Telephone network
- Operations-critical applications and databases
- Supervisory Control and Data Acquisition (SCADA) systems

Even smaller waterworks may have highly automated operations. Maintaining the necessary control to IT platforms may not be adequately addressed. For example, many personal computers (PCs) have direct access to the Internet through modems. Wireless operations present a whole new set of security problems. A recent trend allows for remote access to the SCADA system from an operator's or supervisor's home or other location. An accepted practice of contractors installing SCADA systems is the installation of ethernet cards, whose presence may be unknown to the owner, that allow contractor personnel to upgrade and work on the SCADA system from a remote location and not have to be on site. Hardening of SCADA systems, especially encryption of radio frequency (RF) telemetry may be required. A firewall alone may not be enough so IT security needs to layered.

Disruption to the telephone network is a concern. Depending on the target and its proximity to other utilities, a terrorist attack can cause collateral damage to other infrastructure or utilities in the immediate area. If the telephone network goes down, does a redundant means of communication exist to contact first responders? If landlines go down, is hard-wired SCADA telemetry affected?

Database security also needs layered security. Terminals or PCs having access to employee and customer databases are likely to be connected to at least a local area network (LAN) and have Internet access. Does the public or other employees have access to those buildings or rooms in which the servers (or terminals) are located?

EMPLOYEES concerns include:
- Human Resource Policy
- Personnel Identification
- Personnel Welfare
- Planning and Training

Employees need to be well trained. Training activities need to focus on the employee's role in

security and in how to protect themselves. A known or suspected terrorist WMD attack requires a different response for the employees from how they normally might respond to an emergency. In addition to knowing how to respond to an incident, the operating staff may have to understand alternative means of operating the plant, especially if the SCADA system is no longer functioning or power is lost. If new equipment, such as the standby generator or personal safety equipment is used, do employees know how to properly use and maintain the equipment?

Employees need to understand their role in maintaining security. The new steel door with cyber locks installed does not provide much security if propped open with a brick. Countermeasures that involve people and procedures can be enacted right away to reduce vulnerability. Procedures need to be simple enough to follow and not so disruptive that employees will bypass them to get their job done.

Employees should be identified by distinctive name badges and/or uniforms. Personal means of identification should include a photo ID. Some personal ID cards also have magnetic strips that can be used for access control. Employee uniforms can be colored coded so at a glance one can tell whether the visitor is a mechanic, electrician, operator, or heavy equipment operator.

Human resource policies need to consider whether background investigations (BI) are necessary. Besides privacy concerns are whether the BIs are just for new employees, all employees and if so at what time intervals, cost, delays in hiring and promotions, just operators or personnel with unaccompanied access rights, and what type of BI meets security concerns. Are social security numbers on job applications checked? Witnessed in licensure applications for the trades are the submissions of bogus social security numbers on applications. Investigation reveals that immigrants have paid an agent a fee to assemble all the necessary documents, work visa, etc. Many of these brokers are unscrupulous who provide the immigrants social security numbers of deceased personnel.

When an employee leaves, how is he or she out processed? Are keys collected? Is there an exit interview? Does the interview include a nondisclosure policy? Are uniforms, ID badges, and swipe cards collected? Are vehicle and equipment keys collected? Does the human resource office notify the network administrator so that passwords and access rights are terminated on the last day of work. Is an employee who is discharged for cause processed differently than one who is retiring?

KNOWLEDGE BASE assets include:

- Plans and Planning
- Linkage to Local Law Enforcement Agencies
- Critical Business Documents
- Planning and Training

Knowledge base assets are those needed to be able to function, such as critical business documents and standing operation procedures or emergency response plans. Other people,

besides employees will need access to your knowledge base. Consultants will need access to drawings, specifications, and plans. Contractors also will need certain documents critical to the design and operation of the facility. Often these documents are not accounted for when they go out for requests for proposals. Change of custody documentation and the return of these documents by the unsuccessful bidders provide a measure of security. First responders need access to the knowledge base. Response times may be too long if a relationship is not fostered with local law enforcement, hazmat response teams, fire departments, and emergency medical teams. Coordination with hospital emergency rooms is required because ER personnel may be the first to detect a waterborne disease or illness.

In the event that critical documents are destroyed, backup documents may be needed. Is the location of the duplicate files known and covered in the business recovery plan? If duplicate copies are not available within the utility, consulting engineering firms, contractors, and the regulatory agency may have complete or partial sets of critical documents with their files.

Proper planning will address the above concerns. During an emergency, staff can refer to plans to know who to contact, where to find critical documents and important phone numbers, and procedures to follow. Planning will also identify training needs and performance measures to test in table-top exercises and actual exercises. For example, verify, through testing, that the police can locate remote assets, and get to the site, within the estimated response times.

CUSTOMERS assets include

- Retail Customer Communications
- Interaction with the Press
- Sustainability of Revenue Stream
- Maintenance of Reserves

Customers are important as the primary source of revenue. Business continuity plans need to mitigate consequences and restore service as rapidly as possible. Unless a large cash reserve is maintained, restoring service quickly sustains the revenue stream. If the revenue stream is disrupted, how long will it be before they are out of business? Three weeks? Four weeks? With the customer asset it is important to note the interdependency between the drinking water and wastewater industries especially for billing and source of revenue. Good channels of communication with the customer is important, especially so during an emergency. During any emergency, but especially with a terrorist attack, authorities must portray the image that they are in control. Establishing and maintaining ties with the media can support in this task.

Seeking the assistance of the customer in surveillance is another way that the customer is an asset. Solicit residents living near a remote water storage tank to report any unusual or suspicious activities. If an asset is located along a well traveled jogging path, park lane, or other area visited frequently by joggers, bikers, walkers, and dog owners, signage with a phone to call to report suspicious activity is another way or enlisting customer support.

For the drinking water industry, the first indication that there may be a problem in the distribution system is the customer complaints. The customer better than anyone knows when the water tastes, smells, or appears different. If not already in place, develop and put into place a procedure that responds to customer complaints immediately.

Vulnerability Self Assessment Tool (VSAT)™

After AMSA produced and published its vulnerability checklist, the development of software application program was next. With continued funding from USEPA, AMSA, in collaboration with PA Consulting Group and SCIENTECH, Inc., developed a software application that provides the user with a Vulnerability Self Assessment Tool (VSAT™). The software is flexible, customizable, and user friendly. It is equally applicable to deliberately caused or natural disasters. In addition to a library of prototypical assets included in the software application are threat and countermeasure libraries. As the user proceeds through the self-assessment, the program automatically documents the analysis process during each step. The tool helps the user identify the critical asset(s) and any single points of failures (SPF). The utility of the VSAT™ culminates in a risk-cost report presenting the data in a clear and concise way. This is important, because the goal is business continuity and, at the end of the day, business continues as usual. A detailed overview is located on AMSA's web site at http://www.vsatusers.net/overview.html.

The software tool was made available at no charge to all publicly owned wastewater treatment plants beginning on July 23, 2002. Training on the software, via web cast, becomes available in August. Version 2.0 of VSATwastewater™, VSATwater™, and VSATwaterwastewater™ were distributed in January 2003. Version 2.1 of the software has been released that not only fixed some glitches, but added spreadsheet functionality allowing tables and charts to be produced. For the waterworks who have ordered VSAT, it is important for them to register the software to get library updates and patches.

Vulnerability Assessment Steps

A vulnerability assessment provides security managers the big picture. Regardless of the methodology used, it consists of several steps. We will continue to examine the VSAT methodology. Many large waterworks, serving populations over 100,000 used the Sandia National Laboratories RAM-W^{SM} methodology. (A reminder that the product one is working towards is a risk/cost analysis on which to base decisions and ensure business continuity plan addresses readiness, response, and recovery. The RAM-W^{SM} methodology does not have a financial assessment tool to assist managers in selecting the right bundle of countermeasures for their waterworks.)

The first step is to identify the assets. A "standard" asset listing is provided in the VSAT software, as are a library of potential threats and countermeasures. Assets are grouped into the

categories of Physical, IT, Employee, Knowledge Base, and Customers. In addition to listing all the assets, examples of questions to raise at this time follow. Which assets are critical to business continuity? Which assets can the utility do without? Where are the single points of failure? Which assets, if lost, would not endanger business continuity? Is there functional redundancy? What assets fall on the critical process path? Does an asset have a geographic importance or another way to ask is what percent of demand does this asset represent? Are there critical customers and does something special needed to be done to accommodate their needs. The customer could be a water-dependent industry, a military installation, or a government facility. There are many examples of these in Virginia.

The next step is to identify the threats. This is similar to that done in emergency disaster planning. Threats may be natural disasters or man-made including both internal threats, and external threats. Internal threats include employee and contractor sabotage, theft, and collusion with others. External threats are hackers, theft, low-level vandalism, and terrorist sabotage. The terrorist threat becomes most dangerous when collusion with an insider occurs. One cannot protect against everything. It is best to work towards a specific design basis threat thinking hierarchically. What threat takes the operation down the quickest? What's the easiest target? Where are the interdependencies with other critical assets and infrastructure? For example, access to other potential targets using gravity collectors during low flow as when cyanide was found in the collectors under the US Embassy in Rome. Keep in mind that there may be differences between a target's value as we see it and that from a terrorist's perspective. A war-gaming or "red team" approach has merit in viewing the facility from a terrorist viewpoint.

The third step is to determine each asset's criticality given the threat being evaluated. It is repeated for each asset category. One anticipates the consequence(s) for the asset if it fails or is compromised. Consequences to consider are mission failure and whether loss of life, massive irreversible damage to the environment, widespread destruction of property and or erosion of community wellbeing could occur. One can equate criticality to consequences. In determining whether the waterworks can recover, consideration to severity, duration, and how widespread the consequences might be is envisioned. The VSAT™ software has evaluation tables to assist in determining the criticality and in documenting the analysis.

Once criticality is established, current countermeasures, termed "existing countermeasures" are examined. Countermeasures can deter, detect, delay, decrease response time, and decrease recovery time. One identifies what countermeasure(s) is in place now, and whether its effectiveness has been measured, tested, and maintained. This entails a "walk through" of the facility. Look at whether the staff is trained to use, maintain, or respond to the countermeasure. The value of deterrence has been questioned since it cannot be measured accurately and many in security planning do not rely on it. However, if international terrorists seek an attack option that promises a very high probability of success and low probability of compromise, deterrence may offer our industry greater returns than others. As the target is hardened, the required logistical and financial footprints of the terrorist cell increase to guarantee the same level of success as with a softer target. In wanting to keep the smallest possible footprint and not compromise the

mission, the terrorist may move to a softer target. Countermeasures will be revisited when we try to reduce consequences and vulnerability.

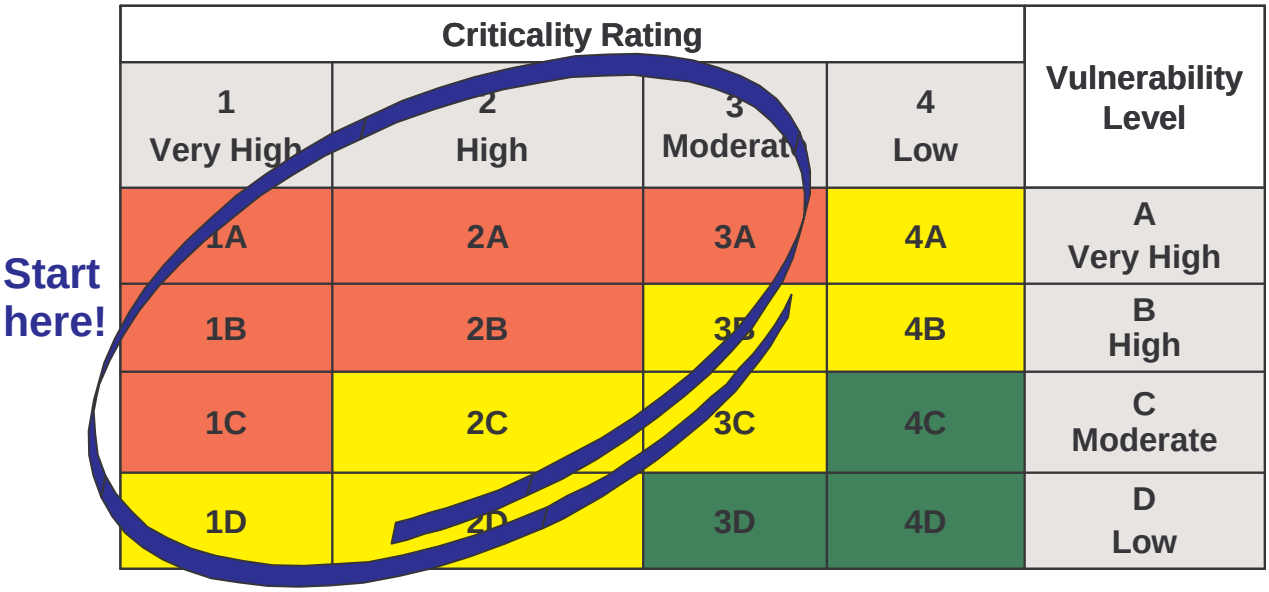
Once existing countermeasures are identified, the process moves to assigning vulnerability. For our purposes, four levels of vulnerability and criticality will be discussed. A very high vulnerability may equate to no ability to survive a threat without failure. If some detection and delay is expected, but the response and recovery is limited or unreliable, the vulnerability is high. A moderate vulnerability has good probable detection and delay, but response and recovery may be slow. A low vulnerability has certain detection and strong delay with fast and reliable response and recovery. Similar to the criticality evaluation described above, the VSAT™ software has evaluation tables to assist in determining the vulnerability and in documenting the analysis. Again, remember that this process is repeated for every asset-threat combination.

Next determine the risk level using a criticality rating found in step three and the vulnerability level. A four by four matrix works well. Across the matrix, from left to right, are the criticality ratings of very high (1), high (2), moderate (3), and low (4). Down the matrix are the vulnerability levels of very high (A), high (B), moderate (C), and low (D). Thus, a 1A has a very high criticality and vulnerability. Conversely, a 4D has a low criticality and vulnerability. Color coding using red (high), yellow (moderate), and green (low) is an effective way to visually recognize the relative risk levels. So, an example, for a low risk level of green, the corresponding criticality levels might be 3D, 4C, and 4D might be an acceptable level of risk for a particular asset. Many may accept moderate risks.

Criticality Rating				Vulnerability Level
1 Very High	2 High	3 Moderate	4 Low	
1A	2A	3A	4A	A Very High
1B	2B	3B	4B	B High
1C	2C	3C	4C	C Moderate
1D	2D	3D	4D	D Low

So those assets with risk levels determined to be high and very high should receive initial emphasis. If using the four by four matrix, start with the high-risk levels (1A, 2A, 3A, 1B, 2B, 3B, 1C, and 2C; criticality/vulnerability) to bring the levels down to an acceptable level. When

trying to reduce relatively low risk assets, we are operating in the realm of diminishing returns and will not receive the risk reduction achieved by working with high-risk assets. We do this by looking at new or potential countermeasures.



Criticality Rating				Vulnerability Level
1 Very High	2 High	3 Moderate	4 Low	
1A	2A	3A	4A	A Very High
1B	2B	3B	4B	B High
1C	2C	3C	4C	C Moderate
1D	2D	3D	4D	D Low

Employing countermeasures can reduce criticality, vulnerability, or both. Besides physical countermeasures, such as perimeter fencing, there are other countermeasures equally or more effective that often incur no or minimal expenses. Most countermeasures that harden an asset will reduce vulnerability. Examples are changing operational procedures, maintaining backup files, and storing duplicate drawings in a separate, secure location. Only a few countermeasures reduce criticality and examples of these are interconnections, alternate power sources, and spares.

The decision as to what constitutes acceptable risk is based on the information that is available on the threat assessment, identification of potential consequences, evaluation of the vulnerabilities, advice on countermeasure effectiveness and cost. Attempting to reduce acceptable risk level to no risk is not practical. There is some level of risk in everything we do on a daily basis. Managers will mostly likely accept a low level of risk for most assets. Some risks can be reduced to low or moderate levels and, unfortunately, there may be some that cannot be reduced at all.

Risk reduction occurs by reducing consequences or reducing vulnerability. Look at countermeasures, in order, that involve people, processes, and technology. Generally solutions involving people and processes are more efficient and less costly. However, expect cultural resistance to changes by staff unless management communicates the reason for the change(s). A security-awareness, training program is effective to do this. Countermeasure activities to

consider include procedural changes; communication and response plans; close coordination with local law enforcement and other first responders; detection and delay systems; IT security; training; and testing of personnel and plans.

The VSAT™ software provides a countermeasure library that gives reference information on considerations for implementing and relative costs and a place to enter the utility specific costs for each countermeasure. Using this software tool provides immediate feedback in seeing the resultant risk reduction for a countermeasure application. The data libraries, provided with the software (including countermeasures) can be customized by the user. So if the default reduction does not reflect conditions on the ground, the user can adjust the value or add a countermeasure not included in the original library. The user also has the option of documenting the rationale for the change in values for future reference. When costs are determined for the various countermeasures under consideration, the user can go back and update cost projections. The software allows the user ease to explore how much reduction results from each countermeasure or multiples of countermeasures.

The next to last step is conducting the benefit and cost analysis. There are several ways to analyze benefit— risk reduction, benefit cost analysis, risk/cost analysis, and regret analysis. Of these, risk/cost analysis is preferred. The approach with this analysis is to achieve the greatest reduction in unit risk for the money invested. The VSAT™ software can greatly assist the security manager in the analysis step and produces a risk/benefit report.

Now, after doing all the assessment and analysis, you want to be ready and you want to be able to respond. Well-crafted business recovery addresses readiness, response, and recovery. In the event that an asset failure occurs, you must have planned and prepared for recovery to continue operations with the least disruption to service as possible. The plan is comprehensive incorporating procedures, personnel, risk/cost-managed capital investments, communications plans, and the other actions needed to answer the following questions: Are they ready? Can they respond? Can they recover?

Depending on the size and complexity of the utility, there is a lot work to do in order to complete the vulnerability assessment requirement. Any methodology used in conducting the vulnerability assessment requires assembling information about the threat, assets, and countermeasures. Although no software can automate all the work required, the availability of a software tool assists in the process. VSAT™ helps to identify potential vulnerabilities, evaluate consequences of those identified vulnerabilities, and document the decision process, rational employed, and relative ranking of risks.

Summary

To protect the water infrastructure in the United States, a need exists to conduct vulnerability assessments. The approach that ODW prefers uses an assessment methodology that is based on assets. The asset categories are: physical assets, information technology platform, employees,

the utility's knowledge base, and customers. This is because a methodology based on assets fit the industry better than traditional methods used by security managers in other industries and requires security specialists to use. Although the requirement to conduct a vulnerability assessment for a waterworks appears daunting and time consuming, the availability of a self-assessment software tool can facilitate the process. As security planning and consequence mitigation is a work in progress, the utility of this software tool will be appreciated in years to come. The software tool can be used to help prepare capital improvement plans, prepare budgets, track improvements in risk reduction, and conduct vulnerability assessments in the out years, when required to do so.

References

Association of Metropolitan Sewage Agencies. (2002) *Asset Based Vulnerability Checklist for Wastewater Utilities,* pp 1-28.

Association of Metropolitan Sewage Agencies. (2002), About VSAT™, http://www.vsatusers.net/about.html

Association of Metropolitan Sewage Agencies. (2002), *About VSAT™ Overview,* http://www.vsatusers.net/overview.html

Combating Terrorism: Threat and Risk Assessments Can Help Priotitize and Target Program Investments (GAO/NSIAD-98-74, April 9, 1998)

Homeland Security – Key Elements of a Risk Management Approach, GAO-02-150T, October 12, 2001

Title IV, PL 107-188*, The Public Health, Security, and Bioterrorism Preparedness and Response Act*

United States Environmental Protection Agency. Instructions to Assist Community Water Systems in Complying with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, Office of Water, EPA 810-B-02-001, January 2003.

Water Environment Federation. (2002) Handout materials and instructor notes, *Wastewater Infrastructure Security Training Workshop,* sponsored by Water Environment Federation through a cooperative agreement with the U.S. Environmental Protection Agency.

White Paper, *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, May 22, 1998*